

EXHIBIT 2

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION**

RowVaughn Wells, Individually and as
Administratrix Ad Litem of the Estate of
Tyre Deandre Nichols, deceased.

Case No. 2:23-CV-02224

Plaintiff,

**STIPULATED ELECTRONIC
DISCOVERY PROTOCOL**

vs.

The City of Memphis, a municipality;
Chief Cerelyn Davis, in her official capacity;
Emmitt Martin III, in his individual capacity;
Demetrius Haley, in his individual capacity;
Justin Smith, in his individual capacity;
Desmond Mills, Jr., in his individual capacity;
Tadarrius Bean, in his individual capacity;
Preston Hemphill, in his individual capacity;
Robert Long, in his individual capacity;
JaMichael Sandridge, in his individual capacity;
Michelle Whitaker, in her individual capacity;
DeWayne Smith, in his individual capacity and
as an agent of the City of Memphis.

Defendants.

STIPULATED ELECTRONIC DISCOVERY PROTOCOL

The Parties hereby agree to the following protocol for production of electronically stored information (“ESI”) and paper (“hard copy”) documents. This protocol governs all production in the matter.

A. Definitions

1. “**Document(s)**” is defined to be synonymous in meaning and equal in scope to the usage of the term in Rule 34(a) of the Federal Rules of Civil Procedure and includes

ESI existing in any medium from which information can be translated into reasonably usable form, including but not limited to email and attachments, word processing documents, spreadsheets, graphics, presentations, images, text files, databases, instant messages, transaction logs, audio and video files, voicemail, internet data, computer logs, text messages, or backup materials. The term "Document(s)" shall include Hard Copy Documents, Electronic Documents, and Electronically Stored Information (ESI) as defined herein.

2. **"Electronic Document(s) or Data"** means Documents or Data existing in electronic form at the time of collection, including but not limited to: e-mail or other means of electronic communications, word processing files (e.g., Microsoft Word), computer presentations (e.g., PowerPoint slides), spreadsheets (e.g., Excel), and image files (e.g., PDF).
3. **"Electronically stored information" or "ESI,"** is information that is stored electronically as files, documents, or other data on computers, servers, mobile devices, online repositories, disks, USB drives, tape or other real or virtualized devices or digital media.
4. **"Hard Copy Document(s)"** means Documents existing in paper form at the time of collection.
5. **"Hash Value"** is a numerical identifier that can be determined from a file, a group of files, or a portion of a file, based on a standard mathematical algorithm that calculates a value for a given set of data, serving as a digital fingerprint, and representing the binary content of the data to assist in subsequently ensuring that data has not been modified and to facilitate duplicate identification. Unless otherwise specified, hash values shall be calculated using the MD5 hash algorithm.
6. **"Load File(s)"** are electronic files containing information identifying a set of paper scanned (static) images or processed ESI and indicating where individual pages or files belong together as documents, including attachments, and where each document begins and ends. Load Files also contain data relevant to individual Documents, including extracted and user-created Metadata, coded data, as well as OCR or Extracted Text. A load file linking corresponding images is used for productions of static images (e.g., TIFFs)
7. **"Metadata"** is the term used to describe the structural information of a file that contains data about the file, as opposed to describing the content of a file.
8. **"Native Format"** means the file format associated with the original creating application and as collected from custodians. For example, the native format of an Excel workbook is an .xls or .xlsx file.
9. **"Optical Character Recognition" or "OCR"** means a technology process that captures text from an image for the purpose of creating an ancillary text file that can be associated with the image and searched in a database. OCR software evaluates

scanned data for shapes it recognizes as letters or numerals.

10. **“Producing Party”** shall refer to the party producing documents or ESI.

11. **“Requesting Party”** shall Refer to the party receiving documents or ESI.

12. **“Searchable Text”** means the native text extracted from an Electronic Document or, when extraction is infeasible, by Optical Character Recognition text ("OCR text") generated from a Hard Copy Document or electronic image.

B. Preservation of ESI

The Parties represent that they have issued litigation hold notices to those custodians with data, and persons or entities responsible for maintenance of non-custodial data, which, based upon then-current information available, are reasonably likely to contain discoverable information.

The Parties agree that the City of Memphis has retained materials that are potentially relevant, including but not limited to materials referenced in preservation letters, Emails, Body-Worn Camera footage and data, Dash Camera Footage and Data, Audio, Mobile Messaging Communications, and Social Media Communications, according to the Memphis Police Department Policy and Procedures, Chapter 11, Section 9, Records Retention.

The Parties agree there is no need to preserve potentially relevant materials from the following sources:

1. Deleted, fragmented, or data in unallocated clusters of storage media that is only accessibly by computer forensics.
2. Volatile random-access memory (RAM), temp files, or other ephemeral data that is difficult to preserve without disabling the operating system or through the use of computer forensics.
3. Temporary internet files, browser history files, cache files, and cookies;
4. Back-up data that a Party knows to be duplicative of ESI, documents, data or tangible things, including metadata about such information, verified to have been retained; and
5. Server, system, or network logs.

Absent a showing of good cause by a Requesting Party, a Producing Party shall not be required to modify the procedures used in the ordinary course of business to back-up and archive data; provided, however, that the Producing Party will act diligently to suspend procedures reasonably anticipated to alter or destroy discoverable data *where such data is not duplicative of data that are more accessible elsewhere and likely to be the sole source of potentially responsive information.*

C. Protocol Does Not Alter Authenticity, Admissibility, or Privilege Status

This Protocol is solely intended to address the format of document productions and does not limit the temporal or substantive scope of discovery.

No Party shall object that ESI produced in Group IV TIFF format is not authentic solely by virtue of changes made in conformance with this Protocol (*e.g.*, use of imaged formats for scanned documents or time normalization of email).

Nothing in this Protocol shall be construed to affect or limit the rights of any Party to make objection as to the authenticity, admissibility, or confidentiality of any document or data.

Nothing in this Protocol shall constitute a waiver by any Party of any claim or privilege or any right to seek protection from or to compel discovery.

Nothing in this Protocol shall be interpreted to limit a Producing Party's right to review documents for relevance, responsiveness, or privilege prior to production.

Nothing in this Protocol shall be interpreted to affect or limit the Protective Order entered in this matter.

Except as expressly set out herein, this Protocol shall not require disclosure of irrelevant information or relevant information protected by the attorney-client privilege or work-product doctrine.

D. eDiscovery Liaison

The Parties agree to designate one or more competent persons to serve as liaisons for purposes of meeting, conferring and attending court hearings regarding the discovery of ESI. Any side is free to change its designated ESI Liaison(s) by providing written notice to the other Parties.

ESI Liaison(s) shall have access to personnel most knowledgeable about the Party's electronic systems and capabilities in order to, as appropriate, answer pertinent questions.

E. Databases and Structured Data

If ESI in commercial or proprietary database formats can be produced in an existing and reasonably usable, delimited report format (*e.g.*, Excel or CSV), the Parties will produce the information in such format.

If an existing report format is not reasonably available or usable, the Parties will meet and confer to attempt to identify a mutually agreeable form of production based on the specific needs and the content and format of data within such structured data source.

F. Hard Copy Documents

Hard copy documents shall be scanned to single page Group IV TIFF format, 300 dpi quality or better with corresponding searchable OCR text. Image file names will be identical to the corresponding Bates numbered images, with a ".tif" file extension. The file name of each text file

should correspond to the file name of the first image file of the document with which it is associated.

All requirements for productions stated in this Protocol regarding productions in TIFF format apply to any production made in JPEG format.

G. Utilizing Documents

In scanning hard copy documents, distinct documents should not be merged into a single record, and single documents should not be split into multiple records (*i.e.*, paper documents should be logically unitized). For example, hard copy documents stored in a binder, folder, or similar container should be produced in the same order as they appear in the container. The front cover of the container should be produced immediately before the first document in the container. The back cover of the container should be produced immediately after the last document in the container. The Parties will undertake reasonable efforts to, or have their vendors, logically unitize documents correctly, and will commit to address situations of improperly unitized documents.

H. Parent-Child Relationships

The Parties agree that if any part of a Document or its attachments is responsive, the entire Document and attachments will be produced, except any attachments that must be withheld or redacted and logged based on privilege or work-product protection.

The Parties shall take reasonable steps to ensure that parent-child relationships within a document family (the association between an attachment and its parent document) are preserved. The child document(s) should be consecutively produced immediately after the parent document. For example, if a Party is producing a hard copy printout of an email with its attachments, the attachments should be processed in order behind the email to the extent reasonably practicable. For further clarification, this shall not require a Party to produce documents merely referenced in responsive documents; provided, however, that documents sent via a link within an email should be produced.

I. Hard Copy Document Metadata

The following metadata fields should be provided for hard copy documents when reasonably available:

1. Beginning Bates number
2. Ending Bates number
3. First attachment Bates number
4. Last attachment Bates number
5. Source location/custodian

6. Confidentiality designation
7. Redacted (Y/N) and
8. Extracted/OCR text file path.

J. Forms of Production

TIFF+ Production

The Parties will produce Electronic Documents, Data and ESI as single page Group IV TIFF images, 300 dpi quality or better, and 8.5"x11" page size, except for documents requiring different resolution or page size with the metadata specified in Addendum A. However, the Parties will produce the following forms of ESI in native formats:

1. Spreadsheets
2. PowerPoint presentations
3. Access databases
4. Delimited text files
5. Photographs
6. Audio and video files
7. Microsoft Word Documents
8. Microsoft Excel Documents
9. Native Email Files
10. Documents of a type which cannot be reasonably converted to useful TIFF images.

All images of documents which contain tracked changes such as comments, deletions and revision marks (including the identity of the person making the deletion or revision and the date and time thereof), speaker notes, or other user-entered data that the source of application can display to the user will be processed such that all that data is visible in the image.

The table below supplies examples of agreed-upon native or near-native forms in which specific types of ESI should be produced:

Source ESI	Native or Near-Native Form or Forms Sought
Microsoft Word documents	.DOC, .DOCX
Microsoft Excel Spreadsheets	.XLS, .XLSX
Microsoft PowerPoint Presentations	.PPT, .PPTX

Microsoft Access Databases	.MDB, .ACCDB
WordPerfect documents	.WPD
Adobe Acrobat Documents	.PDF
Photographs	.JPG, .PDF (with EXIF data supplied in load file if feasible)
E-mail	Messages should be produced in a form or forms that adhere to the conventions set out in the internet e-mail standard, RFC 5322. For Microsoft Exchange or Outlook messaging, .PST format will suffice. Single message production formats like .MSG or .EML may be furnished with folder data. For Lotus Notes mail, furnish .NSF files or convert to .PST. If your workflow requires that attachments be extracted and produced separately from transmitting messages, attachments may additionally be produced in their native forms with parent/child relationships to the message and container(s) preserved and produced in a delimited text file.
Documents that do not exist in native electronic formats or which require redaction of privileged content should be produced in searchable .PDF formats or as single page .TIFF images with OCR text of unredacted content furnished and logical unitization and family relationships preserved.	

K. File Names

Each TIFF image should have a unique file name corresponding to the Bates number of that page with a “.tif” file extension. The file name should not contain any blank spaces and should be zero-padded (*e.g.*, DEF-000001), taking into consideration the estimated number of pages to be produced. If a Bates number or set of Bates numbers is skipped in a production, Producing Party will so note in a cover letter or production log accompanying the production. Bates numbers will be unique across the entire production and prefixes will be consistent across all documents produced.

Producing Party will brand all TIFF images in the lower right-hand corner with its corresponding Bates number without obscuring any part of the underlying image.

Natively produced ESI: A unique Bates number will be assigned to each natively produced document. The filename of each individual document produced shall reflect the Bates number assigned to that document. The Producing Party will also provide the Confidentiality designation

for the document. The metadata fields as set forth in Addendum A will be provided for native documents, as applicable.

L. Extracted Text Files

For each document, a single Unicode text file containing extracted text shall be provided along with the image files and metadata. The text file name shall be the same as the Bates number of the first page of the document. File names shall not have any special characters or embedded spaces. Electronic text must be extracted directly from the native electronic file to the extent reasonably feasible unless the document is an image file or contains redactions, in which case, a text file created using OCR should be produced in lieu of extracted text.

M. Load Files

Productions will, as applicable, include image load files in Opticon or IPRO format as well as Concordance format data (.dat) files with the applicable metadata field identified in Addendum A. All metadata will be produced in UTF-16LE or UTF-8 with Byte Order Mark format.

All native format files shall be produced in a folder named "NATIVE,"

All TIFF images shall be produced in a folder named "IMAGE," which shall contain sub-folders names "0001," "0002," etc. Each sub-folder shall contain no more than 10,000 images. Images from a single document shall not span multiple sub-folders.

All extracted Text and OCR files shall be produced in a folder named "TEXT."

All load files shall be produced in a folder named "DATA" or at the root directory of the production media.

N. Color

Paper documents or redacted ESI that contain color used to convey information (*e.g.*, color coding and highlighting verses merely decorative use) shall be produced as single-page, 300 DPI JPG images with JPG compression set to its highest-quality setting so as not to degrade the original image and/or any other format that does not degrade the original image (*e.g.* PDFs).

O. Redactions

Any redacted material must be clearly labeled on the face of the document as having been redacted and shall be identified as such in the load file provided with the production. Each redacted document shall be produced with an OCR*.txt file containing unredacted text. A document's status as redacted does not relieve the Producing Party from providing all the metadata required herein unless the metadata withheld contains privileged content. The metadata fields in Addendum A will be provided as feasible.

If the items redacted and partially withheld from production are audio/visual files, the Producing Party shall, to the extent reasonably practicable, provide the unredacted portions of the content. If the content is a voice recording, the Parties shall meet and confer to discuss the appropriate manner for the Producing Party to produce the unredacted portion of the content.

P. Privilege Logs

With each production, Producing Party shall supply a log of the documents withheld or redacted under a claim of privilege and/or work product with sufficient information to allow the Receiving Party to understand the basis for the claim within 45 days of each production from which documents are withheld.

The following categories of presumptively privileged documents need not be logged:

1. Communications involving trial counsel that post-date the filing of the complaint;
2. Work product for this action created by counsel, or by an agent of counsel, after letters of preservation were received.
3. Confidential internal communications concerning this action within a law firm or corporate legal department of a corporation or organization.

Q. Deduplication

Global Deduplication. Producing Party may horizontally (globally) de-duplicate documents based on MD5 or SHA-I hash values at the document level or by EDRM MIH/ Message ID and other standard methodology for email within the collection of a custodian or a data source. Attachments to parent documents may not be deduplicated against a duplicate standalone version of the attachment exists, and standalone versions of documents may not be suppressed if a duplicate version exists as an attachment.

Producing Party will track all deduplicated files and provide the names of all custodians of these duplicates of in the load file. If the duplicates are e-mails, the Producing Party must detail the process of creating the hash value, *e.g.*, the names and order on concatenated fields by which the deduplication hash was calculated.

An e-mail message that includes content in the BCC field shall not be treated as a duplicate of a message that does not include content in the BCC field, even if the messages are otherwise identical.

R. De-NISTing

System and application files without user created content (as identified by matching to the NIST National Software Reference Library database) need not be processed, reviewed, or produced. This includes standard system file extensions including BIN, CAB, CHK, CLASS,

COD, COM, DLL DRV, EXE, INF, INI, JAVA, LIB, LOG, SYS and TMP and other filetypes unlikely to contain user generated content.

S. Email Threading

To reduce the volume of entirely duplicative content within email threads, the Parties may, but are not required to, use email threading. A Party may use industry standard message threading technology to remove email messages where the content of those messages, and any attachments, are wholly contained within a later email message in the thread; provided however, that the use of threading must not serve to obscure whether a recipient received an attachment.

T. Production Media

The Producing Party will use the appropriate electronic media (DVD, thumb drive, hard drive or secure FTP transfer) for its ESI production and will endeavor to use the highest capacity suitable media. The Producing Party will label the production media with the name of the Producing Party, production date, media volume name, and Bates number range(s).

Productions on physical media should be encrypted for transmission to the Receiving Party. At the time of production and under separate cover, Producing Party shall furnish decryption credentials to Receiving Party.

U. Social Media and Webpages

To the extent production of social media or webpages is required and where possible, the Parties agree to produce social media as follows:

1. Social Media records shall be collected using industry standard practices, which includes reasonable methods of authentication, including but not limited to MD5 hash values.
2. Social media and webpages will be produced natively, as feasible, or as color TIFF images or JPG images with a searchable, document-level .TXT file of textual content. For ESI from which text cannot be extracted, the Parties agree that they will produce document-level OCR text for each such document.

V. Use of Native Emails and Calendar Items

Parties are prohibited from incorporating Outlook items into any live email environment. This means emails and calendar items that are produced in native format will be uploaded solely and exclusively to the Receiving Party's vendor's databases. Emails and calendar items will be reviewed using the "viewer," "extracted text," "image" rendering in the database, or non-network accessed email applications. Any native review function which would allow the native email or calendar item to be opened in a live, network enabled application must be disabled by the vendor. Nothing herein is intended to prohibit the viewing of native file types other than Outlook items.

W. Time Data Preservation and Normalization

To the extent reasonably practicable, ESI produced in TIFF format shall be processed so as to preserve the date/time shown in the document as it was last saved, *not* the date of collection or processing.

Unless otherwise agreed for ESI produced in TIFF format, all dynamic date and time fields and all metadata pertaining to dates and times in Addendum A, will be normalized to Universal Coordinated Time (UTC). The Parties acknowledge that normalization impacts only dynamic fields and metadata values and does not impact, among other things, dates and times that are hard-coded text with a file. Dates and times that are hard-coded text within a file (for example, in an email thread, dates and times of earlier messages that were converted to body text when subsequently replied to or forwarded; and in any file type, dates and times that are typed as such by users) will be produced as part of the document text in accordance with the provisions herein.

For ESI produced in native formats, system date and time fields shall be preserved and produced as on the system from which it was collected, not the date of collection or processing.

X. Password Protected Files and Processing Exceptions

Producing Party will make reasonable and lawful efforts to ensure that all encrypted or password-protected files are decrypted prior to production and successfully processed so that their content is exposed for indexing, search, review, and production. To the extent that the content of encrypted or password-protected files are decrypted before production and successfully processed and indexed, Producing Party has no duty to identify the encrypted status of such items; however, if items that the Producing Party reasonably believes may contain responsive information cannot be decrypted despite reasonable efforts, Producing Party shall notify Requesting Party about all such items and the Parties will meet and confer in good faith about any next steps.

If ESI fails to properly process for full-text extraction and indexing, Producing Party shall promptly disclose such exceptional file issues to Requesting Party and the Parties shall meet and confer to seek to resolve processing exception unless, after reasonable investigation, the Producing Party has determined that the processing error is not preventing the review of responsive information.

For archive files (zip, jar, rar, gzip, TAR, etc.), all contents should be extracted from the archive with source pathing and family relationships preserved and produced. The fully unpacked archive container file does not need to be included in the production.

Y. Search Methodology

The Parties agree to meet and confer about proposed methods for searching for responsive documents to the extent the Producing Party intends to use keyword search terms or other advanced technologies for identifying responsive documents.

Z. Costs

This protocol shall have no effect on any party's right to seek costs associated with any aspect of discovery, including but not limited to collection, processing, review, or production of documents or ESI.

AGREED:

Dated:

By: /s/
Counsel for Plaintiff

Dated:

By: /s/
Counsel for Defendant City of
Memphis and Cerelyn Davis

Dated:

By: /s/
Counsel for Defendant Emmitt
Martin III

Dated:

By: /s/
Counsel for Defendant
Demetrius Haley

Dated:

By: /s/
Counsel for Defendant Justin
Smith

Dated:

By: /s/
Counsel for Defendant
Desmond Mills, Jr.

Dated:

By: /s/
Counsel for Defendant
Tadarrius Bean

Dated:

By: /s/

Counsel for Defendant Preston
Hemphill

Dated:

By: /s/

Counsel for Defendant Robert
Long

Dated:

By: /s/

Counsel for Defendant
JaMichael Sandridge

Dated:

By: /s/

Counsel for Defendant Michelle
Whitaker

Dated:

By: /s/

Counsel for Defendant
DeWayne Smith

ADDENDUM A

Field Name	Description
BegBates	First Bates identifier of item
EndBates	Last Bates identifier of item
PgCount	Number of pages in the document
FileSize	Size of native file document/email in KB.
FileName	Original name of file as appeared in location where collected
Path	E-mail: Original location of e-mail including original file name. Native: Originating path where native file document was collected including original file name.
NativeLink	Relative path and filename for native file on production media
TextLink	Relative path and filename for text file on production media
AttRange	Bates identifier of the first page of the parent document to the Bates identifier of the last page of the last attachment “child” document
BegAttach	First Bates identifier of attachment range
EndAttach	Last Bates identifier of attachment range
AttachCount	Number of attachments to an e-mail
AttachName	Names of each individual Attachment, separated by semicolons
ParentBates	First Bates identifier of parent document/e-mail message (will not be populated for documents that are not part of a family).
ChildBates	First Bates identifier of “child” attachment(s); may be more than one Bates number listed depending on number of attachments (will not be populated for documents that are not part of a family).
Custodian	E-mail: mailbox where the email resided. Native: Individual from whom the document originated
OtherCustodians	Custodians whose file/message has been de-duplicated; separated by semicolons

From	E-mail: Sender Native: Author(s) of document; separated by semicolons
To	E-mail: Recipient(s); separated by semicolons
CC	E-mail: Carbon copy recipient(s); separated by semicolons
BCC	E-mail: Blind carbon copy recipient(s) separated by semicolons
DateSent (mm/dd/yyyy hh:mm:ss AM)	E-mail: Date and time the email was sent
Subject	E-mail: Subject line of email.
Title	Document: Title provided by user within the document
MsgID	E-mail: “Unique Message ID” field
ModifiedDate (mm/dd/yyyy hh:mm:ss AM)	Document: Last Modified Date and time
CreationDate (mm/dd/yyyy hh:mm:ss AM)	Document: Create Date and time
FileExt	Document: file extension
FileType	Document: file type
Redacted	Denotes that item has been redacted as containing privileged content (yes/no).
Hash	MD5 Hash value of the item
Redacted	Indicator for documents that have been redacted. “Yes” for redacted documents; “No” for un-redacted documents.
HiddenContent	Denotes presence of Tracked Changes/Hidden Content/Embedded Objects in item(s) (Y/N)
Confidential	Denotes that item has been designated as confidential pursuant to confidentiality agreement or protective order (Y/N).

DeDuplicated	Full path of deduplicated instances; separated by semicolons
--------------	--

ADDENDUM B

Agreed Custodian List
Chief CJ Davis
Emmitt Martin
Desmond Mills
Justin Smith
Tadarrius Bean
Preston Hemphill
Dewayne Smith
Robert Long
Jamichael Sandridge
Michelle Whitaker
Former Mayor Jim Strickland
Asst. Chief Shawn Jones
Asst. Chief Don Crowe
Deputy Chief Strategies and Special Projects - Michael Hardy
Deputy Chief Investigative Services - Paul Wright
Deputy Chief Special Operations - Stephen Chandler
Deputy Chief Strategies & Special Projects Division – Michael Hardy
Deputy Chief Information Services - Deputy Chief Joe Oakley
Deputy Chief Administrative Services - Sharonda Hampton
Colonel Training Section – Col. Sharon Cunningham
Deputy Chief Patrol Operations - Samuel Hines

ADDENDUM C

Agreed Search Terms
TBD